Title (en)

METHOD FOR AUTHENTICATING AN ON-CHIP CIRCUIT AND ASSOCIATED SYSTEM-ON-CHIP

Title (de)

VERFAHREN ZUR AUTHENTIFIZIERUNG EINES ON-CHIP-KREISES UND EINES ZUGEHÖRIGEN SYSTEM-ON-CHIP

Title (fr)

PROCÉDÉ D'AUTHENTIFICATION D'UN CIRCUIT SUR PUCE ET SYSTÈME SUR PUCE ASSOCIÉ

Publication

**EP 3809303 A1 20210421 (FR)**

Application

**EP 20200794 A 20201008**

Priority

FR 1911680 A 20191018

Abstract (en)

[origin: CN112685801A] The embodiment of the invention relates to a method for authenticating an on-chip circuit and an associated system-on-chip. An embodiment device comprises a first processing unit configured to process an initial data line and deliver a first processed data line, a first delay unit coupled to the output of the first processing unit and configured to deliver a delayed first processed data line delayed by a first delay, a second delay unit configured to deliver the delayed initial data line delayed by a second delay, a second processing unit coupled to the output of the second delay unit and configured to process the delayed initial data line and deliver a delayed second processed data line, and a comparison unit configured to compare the contents of the delayed first and second processed data lines and deliver a non-authentication signal if the contents are not identical, the first and second delays being equal to a variable value.

Abstract (fr)

Le système sur puce (CI) comprend une entrée (E) pour recevoir une ligne de données initiale (Linit), une première unité de traitement (1) couplée à ladite entrée et configurée pour traiter la ligne de données initiale et délivrer une première ligne de données traitée (LI), des premiers moyens de retard (4) couplés à la sortie de la première unité de traitement et configurés pour délivrer une première ligne de données traitée retardée (L11) d'un premier retard, des deuxième moyens de retard (5) couplées à l'entrée et configurés pour délivrer la ligne de données initiale retardée (Linit_ret) d'un deuxième retard, une deuxième unité de traitement (2) couplée à la sortie des deuxièmes moyens de retard et configurée pour traiter la ligne de données initiale retardée et délivrer une deuxième ligne de données traitée retardée (L2), et des moyens de comparaison (3) configurés pour comparer les contenus des première et deuxième lignes de données traitées retardées et délivrer un signal (S3) de non authentification si lesdits contenus ne sont pas identiques, les premier et deuxième retards étant égaux à une valeur variable.

IPC 8 full level

**G06F 21/75** (2013.01); **G06F 11/16** (2006.01); **G06F 21/70** (2013.01); **G06F 21/71** (2013.01)

CPC (source: EP US)

**G06F 21/44** (2013.01 - US); **G06F 21/755** (2017.08 - EP); G06F 11/1629 (2013.01 - EP); G06F 11/1641 (2013.01 - EP); G06F 11/1695 (2013.01 - EP)

Citation (applicant)

US 2008244305 A1 20081002 - TROPPMANN RAINER [DE], et al

Citation (search report)

- [XI] US 2019171536 A1 20190606 - REFAELI JEHODA [US], et al
- [A] US 2014115401 A1 20140424 - ITO MASAYUKI [JP]
- [AD] US 2008244305 A1 20081002 - TROPPMANN RAINER [DE], et al

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

Designated extension state (EPC)

BA ME

DOCDB simple family (publication)

**EP 3809303 A1 20210421**; **EP 3809303 B1 20230524**; CN 112685801 A 20210420; CN 112685801 B 20240723; FR 3102268 A1 20210423; FR 3102268 B1 20230310; US 11663314 B2 20230530; US 2021117532 A1 20210422

DOCDB simple family (application)

**EP 20200794 A 20201008**; CN 202011117710 A 20201019; FR 1911680 A 20191018; US 202017071094 A 20201015